(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Offenlegungsschrift**

(10) **DE 196 33 802 A 1**

(51) Int. Cl.[6]:
G 07 C 9/00
H 04 L 9/32
// E05B 65/20

(21) Aktenzeichen: 196 33 802.6
(22) Anmeldetag: 22. 8. 96
(43) Offenlegungstag: 26. 2. 98

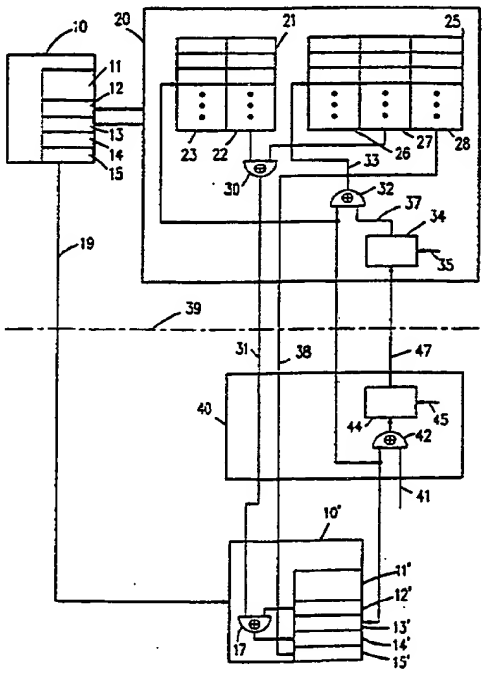
DE 196 33 802 A1

(71) Anmelder:
Philips Patentverwaltung GmbH, 22335 Hamburg, DE

(72) Erfinder:
Buhr, Wolfgang, 22459 Hamburg, DE; Hörner, Helmut, 22549 Hamburg, DE

(54) Verfahren und System zum Einschreiben einer Schlüsselinformation

(57) Bei Schlüsseln, die elektronisch mit einem Objekt, beispielsweise einem Kraftfahrzeug, zusammenarbeiten, tritt manchmal die Notwendigkeit auf, einen neuen Schlüssel herzustellen. Diese Schlüssel sollen an entfernten Stellen schnell zur Verfügung stehen, so daß die für ein Objekt spezifische Schlüsselinformation gesichert übertragen und in den Schlüssel eingeschrieben werden muß. Dazu werden erfindungsgemäß von der entfernten Stelle Objekt-Informationen zu einer zentralen Stelle übermittelt, die die dazu gespeicherte Schlüsselinformation ausliest und mit einer Ident-Information, die sowohl in der zentralen Station als auch in dem Schlüssel gespeichert ist, verschlüsselt und zum Schlüssel übertragen wird. Der Schlüssel kann daraus mit Hilfe der darin gespeicherten geheimen Ident-Information die ursprüngliche Schlüsselinformation zurückgewinnen und abspeichern. Die Ident-Information ist für verschiedene Schlüssel unterschiedlich. Die Objekt-Information wird vor der Übertragung zur zentralen Stelle außerdem mit einer weiteren, auslesbaren Ident-Information verschlüsselt, die ebenfalls im Schlüssel und in der zentralen Stelle gespeichert ist und über die in der zentralen Stelle die geheime Ident-Information zum Verschlüsseln ausgelesen wird. Die verschlüsselte Objekt-Information kann zusätzlich noch verschlüsselt werden, beispielsweise mit einem unsymmetrischen Verschlüsselungs-Algorithmus.



DE 196 33 802 A1

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

BUNDESDRUCKEREI 01. 98 702 069/238

Beschreibung

Die Erfindung betrifft ein Verfahren und ein System zum Einschreiben einer von einer zentralen Stelle gesichert zu einer entfernten Stelle übertragenen Schlüsselinformation in einen dort vorhandenen Datenträger. Bei einer bevorzugten Anwendung ist der Datenträger ein Schlüssel für ein Kraftfahrzeug, wobei der Schlüssel von einem Händler an den rechtmäßigen Besitzer des Kraftfahrzeugs ausgegeben werden soll, beispielsweise weil dieser einen Schlüssel zusätzlich benötigt oder einen ursprünglich beim Kauf des Kraftfahrzeugs empfangenen Schlüssel verloren hat. Es sei jedoch bemerkt, daß das erfindungsgemäße Verfahren bzw. System auch für andere Anwendungsfälle geeignet ist, beispielsweise für Schlüssel für Zugangskontrollen zu bestimmten Räumen oder Bereichen. Mit dem erfindungsgemäßen Verfahren bzw. System können ganz allgemein ausgewählte zugeordnete Informationen gesichert in einen Datenträger eingeschrieben werden.

Wenn eine Schlüsselinformation, die an einer zentralen Stelle gespeichert ist, in einen Datenträger an einer entfernten Stelle eingeschrieben werden soll, muß bei üblichen Systemen verhindert werden, daß die Übertragung der Schlüsselinformation zur entfernten Stelle unberechtigt abgehört werden kann, da sonst ein Betrüger die unberechtigt abgehörte Schlüsselinformation in eigene Datenträger einschreiben kann und damit sich beispielsweise unberechtigt Zugang zu gesicherten Räumen oder Bereichen verschaffen kann. Die andere Möglichkeit, in der zentralen Stelle die Schlüsselinformation in den Datenträger einzuschreiben und diesen dann zu der entfernten Stelle zu versenden, ist auch ungünstig, da der Datenträger beim Transport gestohlen werden kann.

Aufgabe der Erfindung ist es, ein Verfahren zum sicheren Einschreiben einer Schlüsselinformation in einen Datenträger anzugeben, der an einer anderen Stelle als die Stelle, wo die Schlüsselinformation erzeugt wird bzw. gespeichert ist, ausgegeben wird.

Diese Aufgabe wird erfindungsgemäß dadurch gelöst, daß der Schlüssel eine Ident-Information gespeichert enthält, die von außerhalb nicht auslesbar und somit geheim ist, und daß die Schlüsselinformation in der zentralen Stelle mit dieser Ident-Information verschlüsselt und die verschlüsselte Information zum Datenträger an der Ausgabestelle übertragen wird. Im Datenträger wird diese verschlüsselte Schlüsselinformation wieder entschlüsselt und gespeichert.

Dieses Verfahren hat den Vorteil, daß die Datenträger frei versandt werden können, da sie keine Schlüsselinformation enthalten, so daß ein eventueller Dieb die Datenträger nicht benutzen kann. Das unberechtigte Abhören einer übertragenen verschlüsselten Schlüsselinformation ist für einen Betrüger ebenfalls nicht von Nutzen, wenn er nicht einen Datenträger mit der richtigen Ident-Information hat, in die er die verschlüsselte Schlüsselinformation einschreiben könnte.

Dabei ist es wichtig, daß jeder Datenträger eine weitere, offene Ident-Information enthält, die auslesbar ist. Damit ist es dann möglich, daß jeder Datenträger eine individuelle, von anderen Datenträgern unterschiedliche Ident-Information gespeichert enthält, indem die Zuordnung zwischen der weiteren, offenen Ident-Information und der geheimen Ident-Information an der zentralen Stelle gespeichert wird. Mit dieser Maßnahme kann eine verschlüsselte Schlüsselinformation ausschließlich nur von einem, dem richtigen Datenträger richtig entschlüsselt werden.

Um die Zuordnungen von geheimer Ident-Information und Schlüsselinformation sowie der weiteren, offenen Ident-Information leichter organisieren zu können, ist es zweckmäßig, wenn in den Datenträger an einer weiteren Stelle die Ident-Information und die offene Ident-Information eingeschrieben wird, bevor der Datenträger zur entfernten Stelle transportiert wird. Diese weitere Stelle muß dann über eine geschützte Informationsübertragungsverbindung mit der zentralen Stelle gekoppelt sein, damit dort die gleichen Informationen eingeschrieben werden können. Die weitere Stelle kann auch mit der zentralen Stelle identisch sein.

Die zum Datenträger zu übertragende Schlüsselinformation ist wenigstens einem individuellen Objekt, beispielsweise einem Kraftfahrzeug eindeutig zugeordnet. Wenn ein Datenträger einem solchen individuellen Objekt zugeordnet werden soll, muß die dieses Objekt kennzeichnende Objekt-Information zur zentralen Stelle übertragen werden. Um auch diesen Übertragungsweg zu sichern, ist es zweckmäßig, die Objekt-Information vor der Übertragung zur zentralen Stelle mit der weiteren, offenen Ident-Information zu verschlüsseln.

Für die Verschlüsselung von Daten sind eine Vielzahl verschiedener Verfahren bekannt. Bei dem erfindungsgemäßen Verfahren kann als besonders einfache Verschlüsselung und Entschlüsselung der Schlüsselinformation und der Objekt-Information eine Exclusiv-Oder-Verknüpfung mit der Ident-Information verwendet werden. Da die Ident-Information geheim ist, ist selbst bei Kenntnis des Verschlüsselungsverfahrens eine Entschlüsselung ohne Kenntnis der Schlüsselinformation nicht möglich.

Zusätzlich oder auch anstelle der Verschlüsselung mittels Exclusiv-Oder-Verknüpfung kann für die Verschlüsselung der Objekt-Information vor der Übertragung von der entfernten Stelle zur zentralen Stelle noch ein unsymmetrisches Verschlüsselungsverfahren eingesetzt werden, wobei für die Verschlüsselung der Objekt-Information bzw. der verschlüsselten Objekt-Information der offene Schlüssel verwendet wird, während in der zentralen Stelle die Entschlüsselung mit dem geheimen Schlüssel des unsymmetrischen Verschlüsselungsverfahrens durchgeführt wird.

Die Erfindung betrifft ferner ein System zum Einschreiben einer von einer zentralen Stelle gesichert zu einer entfernten Stelle übertragenen Schlüsselinformation in einen dort vorhandenen Datenträger sowie einen Datenträger und ein Terminal zur Verwendung in einem derartigen System.

Ein Ausführungsbeispiel der Erfindung wird nachfolgend anhand der Zeichnung näher erläutert. Darin enthält eine zentrale Stelle 20 zwei Speicher 21 und 25. Der Speicher 21 enthält zwei Gruppen 22 und 23 von Speicherplätzen, die jeweils paarweise einander zugeordnet sind. Durch Aufrufen eines Speicherplatzes der Gruppe 23 mit einer bestimmten Information, nämlich einer offenen Ident-Information eines bestimmten Datenträgers bei Datenträgern mit individuellen unterschiedlichen Ident-Informationen oder der Angabe einer Datenträgergruppe bei Datenträgern mit gruppenweise gleicher Ident-Information, wird diese zugehörige Ident-Information aus dem zugeordneten Speicherplatz der Gruppe 22 ausgelesen.

In entsprechender Weise umfaßt der Speicher 25 in diesem Beispiel drei Gruppen 26, 27 und 28 von Speicherplätzen. In den Speicherplätzen der Gruppe 26 sind Objekt-Informationen gespeichert, und jedem dieser

Speicherplätze ist ein bestimmter Speicherplatz der Gruppe 27 zugeordnet, der eine diesem Objekt zugeordnete Schlüsselinformationen enthält. Ferner sind jedem Speicherplatz der Gruppe 26 vorzugsweise mehrere Speicherplätze der Gruppe 28 zugeordnet, die eine Anzahl Identifiziernummern enthalten. Deren Bedeutung wird später etwas näher erläutert.

An einer weiteren Stelle befindet sich ein Datenträger 10. In der Praxis sind selbstverständlich viele Datenträger vorhanden, die untereinander gleich aufgebaut sind und für die der hier angedeutete Datenträger 10 repräsentativ ist. Dieser Datenträger 10 enthält eine Verarbeitungseinheit 11 und vier Speicherplätze 12 bis 15. Der Speicherplatz 12 dient zum Speichern einer Ident-Information, die nur intern im Datenträger 10 verarbeitet werden kann und in keinem Fall nach außen abgegeben wird. Der Speicherplatz 13 enthält eine den individuellen Datenträger kennzeichnende weitere, offene Ident-Information, die nach außen ausgelesen werden kann. Diese beiden Informationen werden vorzugsweise von der zentralen Stelle 20 geliefert, wo diese beiden Informationen in zwei einander zugeordneten Speicherplätzen der Gruppen 22 und 23 des Speichers 21 eingeschrieben werden, und diese Informationen werden auch an der weiteren Stelle, an der sich der Datenträger 10 zunächst befindet, in die Speicherplätze 12 und 13 eingeschrieben. Die weitere Stelle kann mit der zentralen Station 20 identisch sein.

Dieses Einschreiben in Speicherplätze 12 und 13 erfolgt für eine Vielzahl von Datenträgern, und diese Datenträger werden dann über einen Transportweg 19 zu einer entfernten Stelle transportiert. Dieser Transportweg verläuft zumindest zum Teil über einen nicht geschützten Bereich, der durch die strichpunktierte Linie 39 angedeutet ist. Während dieses Teils des Transportwegs können die Datenträger möglicherweise gestohlen werden. Durch einen solchen Diebstahl kann jedoch kein wesentlicher Schaden entstehen, da die Datenträger noch keine Schlüsselinformation enthalten und somit an keinem Objekt benutzbar sind.

Wenn an der entfernten Stelle in einen Datenträger nämlich in den in der Figur etwas ausführlicher dargestellten Datenträger 10', eine Schlüsselinformation für ein bestimmtes Objekt eingeschrieben werden soll, wird dieser Datenträger 10' mit einem Terminal 40 in Verbindung gebracht. Dadurch wird aus dem Speicherplatz 13' die darin enthaltene offene Ident-Information ausgelesen und über die Verbindung 43 dem Terminal 40 zugeführt. Ferner wird über einen Eingang 41, beispielsweise über eine Tastatur, eine Objekt-Information eingegeben. Diese beiden Informationen werden einer Verschlüsselungsvorrichtung zugeführt, die hier aus zwei Teilen 42 und 44 besteht.

Der Teil 42 der Verschlüsselungsvorrichtung ist hier als Exclusiv-Oder-Verknüpfung ausgeführt. Die verknüpfte Information, die also die mit der offenen Ident-Information verschlüsselte Objekt-Information darstellt, wird einem Teil 44 zugeführt, der eine unsymmetrische Verschlüsselung, beispielsweise nach dem RSA-Verfahren, mit einem festen Schlüssel durchführt, der hier als über einen Eingang 45 zugeführt angedeutet ist. Dieser Schlüssel braucht nicht geheim zu sein, da mit seiner Hilfe eine Entschlüsselung nicht möglich ist.

Die zusätzliche Verschlüsselung mit der offenen Ident-Information bringt eine wesentliche Verbesserung der Sicherheit. Angenommen, die von einer Werkstatt übertragenen Daten, nämlich verschlüsselte Objekt-Information und offene Identinformation wird von einem Betrüger abgehört,der selbst vorprogrammierte Schlüssel besitzt. Wenn dieser Betrüger die gleiche verschlüsselte Objekt-Information überträgt, aber mit der offenen Ident-Information seines Schlüssels, würde er ohne die Verschlüsselung mit der offenen Ident-Information die Schlüsselinformation für das Objekt erhalten, die mit der geheimen Ident-Information seines Schlüssels verschlüsselt ist und somit im Schlüssel richtig entschlüsselt wird, so daß ein gültiger Schlüssel für das Objekt widerrechtlich erhalten wird. Durch die zusätzliche Verschlüsselung mit der offenen Ident-Information wird die vom Betrüger übertragene verschlüsselte Objekt-Information an der zentralen Stelleaber nicht richtig entschlüsselt, so daß die gewünschte Schlüsselinformation nicht aus dem Speicher 25 ausgelesen wird. Wenn der Betrüger aber die ebenfalls abgehörte offene Ident-Information mit überträgt, erhält er lediglich eine Schlüsselinformation, die nicht mit der in seinem Schlüssel gespeicherten geheimen Ident-Information verschlüsselt ist und die also nicht entschlüsselt werden kann. Es ist also nicht möglich, durch Belauschen einer berechtigten Übertragung für ein Objekt Daten zu erhalten,mit denen unberechtigt ein Schlüssel für das gleiche Objekt erzeugt werden kann.

Die vom Teil 44 über die Leitung 47 abgegebene verschlüsselte Information wird nun ebenso wie die offene Ident-Information über die Leitung 43 der zentrale Stelle 20 zugeführt. Diese Übertragung kann über einen nicht gesicherten Weg erfolgen, da die verschlüsselte Information auf der Leitung 47 ohne Kenntnis des geheimen Schlüssels der unsymmetrischen Verschlüsselung nicht entschlüsselt werden kann und die offene Ident-Information keinen direkten Hinweis auf die im Datenträger benötigte Schlüsselinformation enthält.

In der zentralen Stelle 20 wird die verschlüsselte Information auf der Leitung 47 einer Entschlüsselungsvorrichtung zugeführt, die die Teile 32 und 34 umfaßt. Im Teil 34 wird eine Entschlüsselung der über die Leitung 47 übertragenen Information durchgeführt, und zwar mit Hilfe eines geheimen Schlüssels, der hier über einen Eingang 35 zugeführt angedeutet ist. Am Ausgang 37 des Teils 34 der Entschlüsselungsvorrichtung liegt dann die gleiche Information vor wie am Ausgang der Exclusiv-Oder-Verknüpfung 42 im Terminal 40. Dies ist jedoch noch nicht die über den Eingang 41 des Terminals 40 zugeführte Objekt-Information. Daher führt die Leitung 37 auf eine Exclusiv-Oder-Verknüpfung 32, die an einem weiteren Eingang die offene Ident-Information über die Leitung 43 erhält. Am Ausgang 33 der Exclusiv-Oder-Verknüpfung 32 liegt nun die entschlüsselte Objekt-Information vor, mit der der Speicher 25 angesteuert wird. Dabei wird in der Gruppe 26 der Speicherplatz ausgewählt, der diese Objekt-Information enthält, und aus dem zugehörigen Speicherplatz der Gruppe 27 wird die Schlüsselinformation ausgelesen.

Ferner wird mit Hilfe der offenen Ident-Information auf der Leitung 43 der Speicher 21 angesteuert, indem der Speicherplatz der Gruppe 23 aufgesucht wird, der diese Ident-Information enthält, und der zugehörige Speicherplatz der Gruppe 22, der die geheime Ident-Information enthält, wird ausgelesen.

Die aus dem Speicher 21 und dem Speicher 25 ausgelesene Information wird einer Verschlüsselungsanordnung 30 zugeführt, die hier ebenfalls als Exclusiv-Oder-Verknüpfung ausgeführt ist. Die an deren Ausgang 31 auftretende Information wird nun zur entfernten Stelle übertragen, wobei der Übertragungsweg nicht sicher sein muß, da die entschlüsselte Schlüsselinformation aus

der Information auf der Leitung 31 nur mit Hilfe der richtigen geheimen Ident-Information zu gewinnen ist, die jedoch im Datenträger verborgen gespeichert ist und nicht direkt übertragen wird.

Im vorliegenden Beispiel wird aus dem Speicher 25 außerdem noch aus einem zugeordneten Speicherplatz der Gruppe 28 eine Identifiziernummer ausgelesen und über die Leitung 38 zur entfernten Stelle übertragen, wobei ebenfalls ein ungesicherter Weg verwendet werden kann.

In der entfernten Stelle werden die Informationen auf der Leitung 31 und der Leitung 38 über das Terminal 40 dem Datenträger 10' zugeführt. Die Identifiziernummer auf der Leitung 38 wird im Datenträger 10' direkt in den Speicherplatz 15' eingeschrieben, während die verschlüsselte Schlüsselinformation auf der Leitung 31 einer Entschlüsselungsvorrichtung 17 zugeführt wird, die an einem weiteren Eingang die geheime Ident-Information aus dem Speicherplatz 12' erhält. Diese Entschlüsselungsvorrichtung ist wieder als Exclusiv-Oder-Verknüpfung ausgeführt und gibt somit am Ausgang die entschlüsselte Schlüsselinformation ab, die in den Speicherplatz 14' eingeschrieben wird. Damit enthält der Datenträger 10' nun alle für seine Benutzung bei einem bestimmten Objekt, beispielsweise bei einem Kraftfahrzeug, notwendigen Informationen, ohne daß die entscheidend wichtige Schlüsselinformation bei der Übertragung auf unberechtigte Weise ermittelt werden kann.

Die Identifiziernummer im Speicherplatz 15' ist für das beschriebene Verfahren nicht unbedingt notwendig und dient, wenn der Datenträger ein Schlüssel für ein Kraftfahrzeug ist, dazu, daß im Kraftfahrzeug zunächst über diese Identifiziernummer geprüft wird, ob es sich um einen zulässigen Schlüssel handelt, bevor mit Hilfe der Schlüsselinformation geprüft wird, ob es sich um einen berechtigten Schlüssel handelt. Wenn nämlich mit einem nicht berechtigten Schlüssel, d. h. mit einer falschen Schlüsselinformation, eine Anzahl Startversuche durchgeführt worden sind, werden alle Funktionen des Kraftfahrzeugs dauerhaft blockiert, wobei die Blockierung nur mit einer bestimmten, geheimen Prozedur aufgehoben werden kann. Durch die Identifiziernummer wird also verhindert, daß mit einem falschen Schlüssel, der z. B. zu einem anderen Kraftfahrzeug gehört und somit selbstverständlich eine andere Schlüsselinformation enthält, als gültig erkannte Fehlversuche durchgeführt werden können.

Zweckmäßig enthält jeder für ein Kraftfahrzeug berechtigte Schlüssel eine andere Identifiziernummer, und dafür sind im Speicher 25 zu jeder Objekt-Information und ebenso in dem zugehörigen Objekt eine Anzahl Identifiziernummern gespeichert.

Es ist klar, daß die Verschlüsselung im Terminal 40 mit Hilfe der Teile 42 und 44 und die entsprechende Entschlüsselung in der zentralen Stelle auch auf andere Weise als beschrieben durchgeführt werden kann. Wichtig ist, daß die Information auf der Leitung 47 in einer Weise verschlüsselt ist, die eine Entschlüsselung nur durch übertragene Informationen nicht möglich macht.

Patentansprüche

1. Verfahren zum Einschreiben einer von einer zentralen Stelle gesichert zu einer entfernten Stelle übertragenen Schlüsselinformation in einen dort vorhandenen Datenträger, der nach dem Einschreiben einem ausgewählten von mehreren Objekten über die Schlüsselinformation eindeutig zugeordnet ist und der eine nach außen nicht abgebbare Ident-Information sowie eine weitere, offene Ident-Information, die auslesbar ist, gespeichert enthält, die einander zugeordnet auch in der zentralen Stelle gespeichert sind, wobei zunächst eine das individuelle Objekt kennzeichnende Objekt-Information zur zentralen Stelle übertragen wird, dort die zur Objekt-Information gespeicherte Schlüsselinformation ausgelesen und mit der Ident-Information verschlüsselt und zum Datenträger übertragen und im Datenträger mit der darin gespeicherten Ident-Information entschlüsselt und die entschlüsselte Schlüsselinformation gespeichert wird.

2. Verfahren nach Anspruch 1 wobei in den Datenträger an einer weiteren Stelle, die über eine geschützte Informationsübertragungsverbindung mit der zentralen Stelle gekoppelt ist, die Ident-Information und die weitere, offene Ident-Information vor dem Transport des Datenträgers zur entfernten Stelle eingeschrieben wird und diese Ident-Information auch an der zentralen Stelle gespeichert wird.

3. Verfahren nach Anspruch 2, wobei die Objekt-Information vor der Übertragung zur zentralen Stelle mit der offenen Ident-Information verschlüsselt wird.

4. Verfahren nach einem der Ansprüche 1 bis 3, wobei die Verschlüsselung und Entschlüsselung der Schlüsselinformation und der Objekt-Information durch eine Exclusiv-Oder-Verknüpfung mit der weiteren, offenen Ident-Information erfolgt.

5. Verfahren nach Anspruch 3, wobei die verschlüsselte Objekt-Information vor der Übertragung durch ein unsymmetrisches Verschlüsselungsverfahren mit den diesem zugeordneten öffentlichen Schlüssel zusätzlich verschlüsselt wird und in der zentralen Stelle mit dem geheimen Schlüssel des Verschlüsselungsverfahrens entschlüsselt wird.

6. System zum Einschreiben einer von einer zentralen Stelle gesichert zu einer entfernten Stelle übertragenen Schlüsselinformation in einen dort vorhandenen Datenträger, der nach dem Einschreiben einem ausgewählten von mehreren Objekten über die Schlüsselinformation eindeutig zugeordnet ist, wobei die zentrale Stelle einen ersten Speicher, der wenigstens eine Ident-Information und eine zugeordnete weitere Ident-Information sowie für jedes der mehreren Objekte eine das Objekt keimzeichnende Objekt-Information und die dem Objekt zugeordnete Schlüsselinformation enthält, und eine Verschlüsselungsanordnung zum Verschlüsseln einer aus dem ersten Speicher ausgelesenen Schlüsselinformation mit der Ident-Information sowie eine Übertragungsanordnung zum Übertragen der verschlüsselten Schlüsselinformation an die entfernte Stelle umfaßt, und wobei der Datenträger einen zweiten Speicher, der einen ersten Speicherplatz für eine Ident-Information, einen zweiten Speicherplatz für eine Schlüsselinformation und einen dritten Speicherplatz für eine den Datenträger kennzeichnende weitere Ident-Information enthält, sowie eine Entschlüsselungsvorrichtung umfaßt, die mit einem Informationseingang des Datenträgers und mit dem ersten Speicherplatz verbunden ist, um nach Empfang einer verschlüsselten Schlüsselinformation eine entschlüsselte Schlüsselinformation abzugeben und in den zweiten Speicher-

platz einzuschreiben.

7. System nach Anspruch 6, wobei an der entfernten Stelle ein Terminal vorgesehen ist, mit dem der Datenträger koppelbar ist, um das Auslesen der weiteren Ident-Information auszulösen und diese weitere Ident-Information an die zentrale Stelle zu übertragen und die danach von der zentralen Stelle übertragene verschlüsselte Schlüsselinformation zu empfangen und an den Datenträger zu übertragen.

8. System nach Anspruch 7, wobei das Terminal eine Verschlüsselungsvorrichtung enthält, um eine eingegebene Objekt-Information mit der Ident-Information und/oder mit der weiteren Ident-Information zu verschlüsseln und an die zentrale Stelle zu übertragen, und die zentrale Stelle eine Entschlüsselungsvorrichtung enthält, um die empfangene verschlüsselte Objekt-Information mittels der ebenfalls übertragenen weiteren Ident-Information zu entschlüsseln und mit der entschlüsselten Objekt-Information den ersten Speicher anzusteuern und die zugeordnete Schlüsselinformation auszulesen.

9. System nach einem der Ansprüche 6 bis 8, wobei die Verschlüsselungsvorrichtung in der zentralen Stelle und die Entschlüsselungsvorrichtung im Datenträger als Exclusiv-Oder-Verknüpfungselement aufgebaut sind.

10. System nach Anspruch 8 oder 9, wobei die Verschlüsselungsvorrichtung im Terminal eingerichtet ist, die verschlüsselte Objekt-Information zusätzlich mit dem öffentlichen Schlüssel einer unsymmetrischen Verschlüsselung zusätzlich zu verschlüsseln und an die zentrale Stelle zu übertragen und die Entschlüsselungsvorrichtung in der zentralen Stelle eingerichtet ist, um die empfangene zusätzlich verschlüsselte Objekt-Information mit dem geheimen Schlüssel der unsymmetrischen Verschlüsselung und mit der ebenfalls empfangenen weiteren Ident-Information zu entschlüsseln und die entschlüsselte Objekt-Information an den ersten Speicher abzugeben.

11. Datenträger zur Verwendung in einem System nach einem der Ansprüche 6 bis 10, mit einer Entschlüsselungsvorrichtung und einem Speicher mit einem ersten Speicherplatz zum Speichern einer Ident-Information und einem zweiten Speicherplatz zum Aufnehmen einer Schlüsselinformation, wobei die Entschlüsselungsvorrichtung mit dem ersten Speicherplatz gekoppelt ist, um eine empfangene verschlüsselte Schlüsselinformation mittels der aus dem ersten Speicherplatz ausgelesenen Ident-Information zu entschlüsseln und die entschlüsselte Schlüsselinformation in den zweiten Speicherplatz einzuschreiben, und wobei das Ausgeben der Ident-Information aus dem Datenträger gesperrt ist.

12. Datenträger nach Anspruch 11, wobei der Speicher einen dritten Speicherplatz zum Aufnehmen einer weiteren Ident-Information aufweist, und der Speicher von außerhalb des Datenträgers ansteuerbar ist, um die weitere Ident-Information aus dem Speicher nach außen abzugeben.

13. Datenträger nach einem der Ansprüche 11 oder 12, wobei die Entschlüsselungsvorrichtung als Exclusiv-Oder-Verknüpfungselement ausgebildet ist.

14. Terminal zur Verwendung in einem System nach einem der Ansprüche 6 bis 10, mit einer Koppelvorrichtung für einen Datenträger, einer Übertragungsvorrichtung für Informationen, einer Eingabevorrichtung zum Eingeben von Informationen und einer Verschlüsselungsvorrichtung mit zwei Eingängen, die mit der Eingabevorrichtung und der Koppelvorrichtung verbunden sind, und einem Ausgang, der mit der Übertragungsvorrichtung verbunden ist, um eine über die Eingabevorrichtung eingegebene Objekt-Information mit einer über die Koppelvorrichtung zugeführte Ident-Information zu verschlüsseln und die verschlüsselte Objekt-Information an die Übertragungsvorrichtung abzugeben.

15. Terminal nach Anspruch 14, wobei die Verschlüsselungsvorrichtung jeweils dazu eingerichtet ist, die verschlüsselte Objekt-Information zusätzlich mit dem öffentlichen Schlüssel einer unsymmetrischen Verschlüsselung zu verschlüsseln und nur die zusätzlich verschlüsselte Objekt-Information an die Übertragungsvorrichtung abzugeben.

Hierzu 1 Seite(n) Zeichnungen

Nummer: DE 196 33 802 A1
Int. Cl.[6]: G 07 C 9/00
Offenlegungstag: 26. Februar 1998